

RECEIVED
CENTRAL FAX CENTER

OCT 04 2006

Serial No. 09/468,377
Art Unit No. 2134REMARKS

Claims 1-20 are pending in the patent application. The Examiner has rejected Claims 9, 14 and 17 under 35 USC 112 as indefinite. By this amendment, the language of Claims 9, 14, and 17 has been amended to address the rejection. The Examiner has also rejected Claims 1, 5, and 9 as indefinite. The Examiner states that it is unclear to the examiner how the encrypted second key may be decrypted by using only the one time password and not also using the first key. Applicants respectfully assert that the user only needs the second key for decrypting the encrypted version of the data, as is well known in the relevant art, such as in the Diffie-Hellman approach wherein a party needs only 2 of the 4 pieces of the keys, such that the client knows its own secret key "a" and only needs g^b from the content provider to be able to calculate the key. The Examiner also states that it is unclear as to how the client would not know the value of b. Applicants are not claiming that the client would not know the value of b, but the client need not know the value of b in order to determine the key. Applicants

Y0999-558

-17-

Serial No. 09/468,377

Art Unit No. 2134

believe that the claim language is definite and well supported by the specification and the background art.

With regard to the rejections of Claims 9, 14 and 17 based on the recitation of "wherein an encryption key K_{ab} ... uses $g^{(a*b)}$ ", Applicants have amended the claim language to clarify that the encryption key is used to encrypt and decrypt the data, including encrypting/sealing $g^{(a*b)}$.

The Examiner has rejected Claims 1, 3-4, 7-8, 12 and 15 under 35 USC 103 as unpatentable over the teachings of Thomlinson in view of Aziz; Claims 2, 5-6, 13, 16, and 18-19 as unpatentable over Thomlinson in view of Aziz and further in view of Mi; Claims 9, 14, and 17 as unpatentable over Thomlinson in view of Aziz and Jablon; Claims 10 and 20 as unpatentable over Thomlinson in view of Aziz and Jablon and further in view of Mi; and, Claim 11 as being unpatentable over the teachings of Thomlinson in view of Aziz, and Jablon and further in view of Schneier. For the reasons set forth below, Applicants respectfully assert that all of the pending claims are patentable over the cited prior art.

The present invention is a computer program product and method for securely providing data of a content provider to a user without trusting an internet service provider. The

YO999-558

-18-

Serial No. 09/468,377
Art Unit No. 2134

present invention allows secure data transfer between a content provider and a user without having the internet service provider participate in the security features, such that transmitted data is always encrypted. In that way, a user could access the internet through any service provider, without sharing any security information with the internet service provider. Similarly, the content provider could securely transmit encrypted data to a trusted user, without concern that the internet service provider, or other customers of the internet service provider, could access the content provider's data. The security relationship is between the content provider and the user and the claims expressly recite steps for exchanging encryption keys and passwords only between the user and the content provider. By the previous amendments, Applicants have ensured that all of the claims expressly recite that the content provider is not the internet service provider and that the secure transmission is done without trusting the internet service provider.

Claims 5-8, 13, 16 and 19 recite a method, program storage device and means for securely providing data of a content provider through an internet service provider to a

YO999-558

-19-

Serial No. 09/468,377
Art Unit No. 2134

user at a client machine without trusting an internet service provider, wherein the content provider and the internet service provider are different entities, the method comprising, when the user accesses a web page of the content provider, downloading an applet from the content provider to the client machine; generating a first key known only to the content provider; encrypting a second key using the first key and an encryption algorithm requiring a one-time password; transmitting the second encrypted key for storage at the client machine; and when the user first desires to access the data, the applet requesting the one-time password from the user and, based on correct entry of the one-time password, decrypting said second encrypted key and accessing the data by decrypting an encrypted version of the data at the client machine using the second key. Support for the added features related to downloading and executing the applet is found in the Specification (e.g., at page 6, line 12, and page 7, lines 3-21).

Claims 9-11, 14, 17, and 20, recite a method, program storage device and means for authenticating a user at one client machine seeking access to secure data of a content provider comprising: transmitting g^a and the identity of

YO999-558

-20-

Serial No. 09/468,377
Art Unit No. 2134

the user of the one client machine to the content provider node, wherein g and a are random numbers and where a is known only to the client machine, and where g is known to both content provider and the client machine; generating g^b , where b is known to the content provider node but need not be known to the client; encrypting g^b with a one-time password of the user and transmitting g^b to the client machine; at the client decrypting g^b ; generating encryption key K_{ab} using a and g^b ; calculating $g^{(a*b)}$ using the one-time password to decrypt g^b ; and encrypting and transmitting $g^{(a*b)}$ to the content provider, whereby the client machine's knowledge of $g^{(a*b)}$ authenticates the user to the content provider. Support is found in the original Specification (see: e.g., page 9).

The Examiner has rejected all of the pending claims using the Thomlinson patent as the primary reference. Thomlinson patent is directed to a system and method for protecting data wherein the service provider is involved in the encryption and authentication process. As expressly stated in Col. 2, lines 12-13 of Thomlinson, "encryption is based on the user's logon password or some other secret supplied during network logon." Applicants contend that the

YO999-558

-21-

Serial No. 09/468,377
Art Unit No. 2134

security relationship in the Thomlinson patent is not between a user and a content provider wherein the content provider is a different entity from the service provider. Applicants respectfully assert that the present invention expressly omits the service provider from the process in order to protect data when an untrusted service provider is part of the data delivery.

The Thomlinson system provides a master key which is used to encrypt an item key (col. 9, lines 20-22). In turn, at the "client" in Thomlinson, the master key is used to decrypt the item key (Col. 10, lines 5-13). Clearly, the master key is known to both entities. Moreover, Applicants point out that Thomlinson teaches the generation of the first key on the server with an already authenticated login. The present invention avoids the creation of a first key on a trusted server under authenticated login, and instead creates the first key by protocol exchange between peers without trusting the service provider and/or communication media. Thomlinson consistently uses a central server with an established login (page 2, line 13-15).

The Examiner concludes that the item key of Thomlinson reads on the second key. However, Thomlinson states at Col.

YO999-558

-22-

Serial No. 09/468,377

Art Unit No. 2134

9, lines 13-27 that "an item key is randomly generated for each data item received...[and]...[t]he data item is encrypted with its corresponding item key...using a master key." Further, "the master key is encrypted using a code that is derived from user authentication." Clearly what Thomlinson is teaching is encryption based on user identification at logon, using an encryption algorithm which was previously determined (see: Col. 8, lines 64-67), and assignment of item "keys", which are not encryption or decryption keys but are item identifiers that are encrypted along with the items. Clearly Thomlinson is not teaching or suggesting generating first and second keys as claimed. Thomlinson explicitly requires a trusted server (Col. 2, lines 10-15) through a previous login/password interaction. Further, Thomlinson explicitly states that "all encryption and decryption, item integrity checks, and user authentication are performed by the server" (Col. 2, line 20) such that the server must be trusted. Applicants further contend that the fact that Thomlinson generates a master key by its trusted server (Col. 9, line 20) does not anticipate or obviate the claimed invention since the claimed invention expressly engages in a one-time

YO999-558

-23-

Serial No. 09/468,377
Art Unit No. 2134

peer-to-peer communication (i.e., using the one-time password) to establish the secure trust relationship between the client and the content provider without having to use the Thomlinson login authentication of a service provider between the client and the content provider.

Applicants further note that the Thomlinson system will not work without a trusted server, since it provides no peer-to-peer authentication without using the trusted server. To suggest modifying Thomlinson in a manner that will render it inoperable for its stated objective is untenable.

The Examiner has acknowledged that Thomlinson lacks any mention of a one-time password and has cited the Aziz patent teachings. Applicants reiterate that Aziz does not provide those teachings which are missing from the Thomlinson patent. Aziz does not teach encrypting a second key using a first key and a one time password at one entity and then decrypting the second encrypted key using the one time password at the other entity.

With regard to Claims 2 and 6, the Examiner has further cited the Mi patent in combination with Thomlinson and Aziz; and, in rejecting Claim 10, the Examiner has cited Mi in

YO999-558

-24-

Serial No. 09/468,377

Art Unit No. 2134

combination with Thomlinson, Aziz and Jablon. The Mi patent is directed to a system and method for using an internet-based caller ID to control client access to an object stored on a server. Under the Mi method, upon receipt of a client request, the server generates a DLL file 407 having a secret key 418 (Col. 7, lines 23-26) and sends the DLL file with an applet to the client browser (Col. 7, lines 27-33 and 41-44). At the client, the DLL file is executed so that the client uses the same secret key 418 from the DLL file, as well as its processor number 422 which is known to the server (Col. 6, lines 56-67) to calculate a hash value which is returned to the server (Col. 8, lines 4-9 and 32-35). When the server receives the hash value from the client, the server's comparison agent calculates a hash value, compares it to the received hash value, and allows the client access to the data if the two values compare favorably (Col. 8, lines 36-44). For each session, the DLL file will contain a different secret key (Col. 7, lines 26-27 and Col. 8, lines 49-53) which is known to both the server and the client.

Applicants contend that the resulting combination would not obviate the invention as claimed. Since both Thomlinson

YO999-558

-25-

Serial No. 09/468,377
Art Unit No. 2134

and Mi have a key that is known to both entities, there is neither a teaching nor a suggestion of generating and using a key that is known to one entity but not known to that other. Moreover, neither reference, alone or in combination with the additionally-cited art, provides for the accessing of data as claimed or the downloading and use of an applet. While Mi may have the processor number known to the server, Mi does not teach or suggest the use of that information for permitting data access only on one client machine.

With regard to Claims 9, 14 and 17, Applicants disagree with the Examiner's conclusion that the claim language is obviated by the combination of Thomlinson, Aziz and Jablon. Applicants respectfully rely on the arguments set forth above with regard to the teachings of the Thomlinson patent, alone and in combination with Aziz. The Thomlinson patent simply does not teach that a key is known only to one entity. Moreover, the teachings cited from the Jablon patent, from Col. 7, lines 16-27, do not provide those teachings which are missing from Thomlinson and Aziz. What Jablon teaches is that a user creates "the user's hidden password, which is maintained as a shared secret and stored securely with the host" (see: Col. 7, lines 18-20).

YO999-558

-26-

Serial No. 09/468,377
Art Unit No. 2134

Therefore, the password is known to both the user and the host. Clearly Jablon is not providing the teachings which are missing from the Thomlinson and Aziz patents.

In rejecting Claim 11, the Examiner has also cited the Applied Cryptography reference for its teachings regarding MAC authentication procedures. Applicants respectfully assert that the reference does not provide the teachings which are missing from the Aziz, Thomlinson and Jablon patents. Moreover, Applicants contend that the Examiner has failed to show how the MAC authentication procedures would be integrated into the teachings of the combined references. The Examiner concludes that "[b]oth client and server generate the same key during the authentication procedure so the MAC authentication would be an easy way to check authenticity without needing security". Applicants disagree with the Examiner's conclusion. Moreover, applying a MAC to Thomlinson, alone or in combination with the additionally-cited patents, would not result in the invention as claimed, since none of the cited references teaches or suggests the use of keys not known to the other party, etc.

YO999-558

-27-

RECEIVED
CENTRAL FAX CENTER

OCT 04 2006

Serial No. 09/468,377

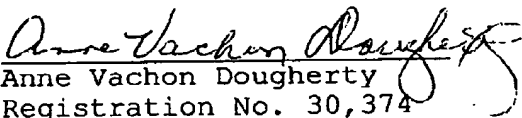
Art Unit No. 2134

Applicants respectfully assert that the Examiner has not established a *prima facie* case of obviousness, since the Examiner has not provided prior art which teaches or suggests all of the claims limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)).

Based on the foregoing remarks, Applicants respectfully request entry of the amendments, reconsideration of the claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

Y. Baransky, et al

By: 
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910